Security Testing Report

IGT_Devices\Coronary

Guided Health Service- GHS_1.1.5.0

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

Table of Contents

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

Document Version Control

Name of the document : Guided Health Service- GHS 1.1.5.0 Security Testing Report		
Version: 1.0	**Intake ID:**	2850
Document Definition: This document highlights the vulnerabilities currently existing in the application under scope. It also documents possible actions to be taken to reduce/eliminate the vulnerabilities.	**Document ID:**	PRHC/C40/SVN/89080
Author: Sai Praneetha Bhaskaruni	**Effective Date:**	15/Dec/2023
Reviewed by: Chaitra N Shivayogimath		

Document History

Version	Date	Author	Section	Changes
0.1	14 Dec 2023	Sai Praneetha Bhaskaruni	Complete	Initial Draft
1.0	15 Dec 2023	Chaitra N Shivayogimath	Complete	Final Review

Distribution List

User/Department/Stakeholder	E-Mail ID
Project Owner and PSO	smita.bansal@philips.com; Chandrashekar.Natarajan@philips.com; Priya.Vijayachandran@philips.com; sreenath.kooloth@philips.com

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

1. Definitions & Abbreviations

Term	Explanation
SCoE	Security Center of Excellence
TLS	Transport Layer Security
SSL	Secure Socket Layer
XSS	Cross Site Scripting
JWT	Json Web Token
CORS	Cross Origin Resource Sharing

The severity of every vulnerability has been calculated by using industry standard **Common Vulnerability Scoring System (CVSS)** used for assessing the severity of computer system vulnerabilities. CVSS provides a way to capture the principal characteristics of a vulnerability and produce a numerical score (Scores range from 0 to 10, with 10 being the most severe) reflecting its severity. The numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organization properly assess and prioritize their vulnerability management processes.

The severity rating for the numerical values are mapped below

None	0.0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

The **Severity** and **CVSS vector** of each vulnerability is calculated using the CVSS V3 **Base Score Metrics** Calculator located here. Vulnerabilities identified during security assessment are classified into standardized categories. Refer following table for more information:

Categories for vulnerability classification

Web application security assessment	OWASP Top Ten - 2021
Mobile application security assessment	OWASP Top Ten - 2016
IoT/Hardware security assessment	OWASP Top Ten - 2014

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

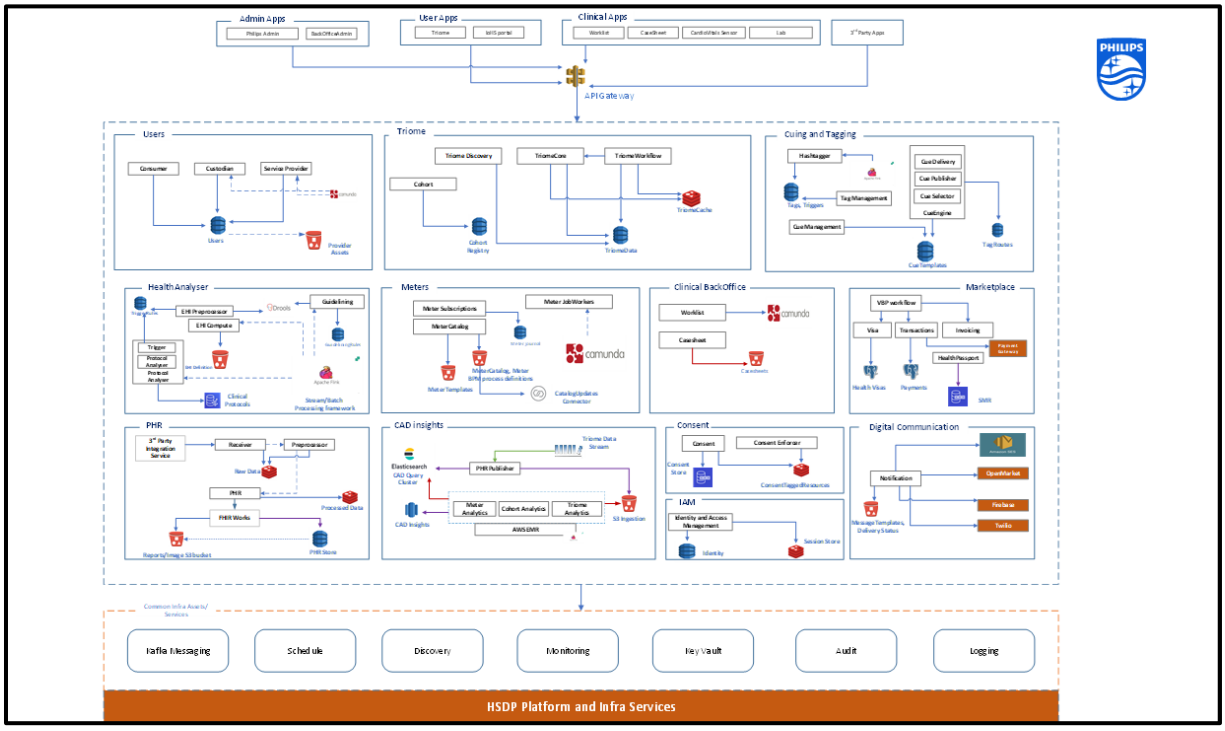
2. System Details & Architecture

A Conceptual Overview of CAD GHS Web application:

- Engages consumers towards their cardiac health through monitoring, forecasting and guide-lining
- A proactive health services marketplace (B2C and B2B) backed by outcome-based services (meters)
- Post MVP, expand the solution to assurance services for large cohorts based on protocol-based clinical guidance and AI-driven differential diagnosis

Test Environment: Validation

Architecture Diagram:



This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

Payment - Phase I

To enable payment for subscriptions and make it available for Consumers.

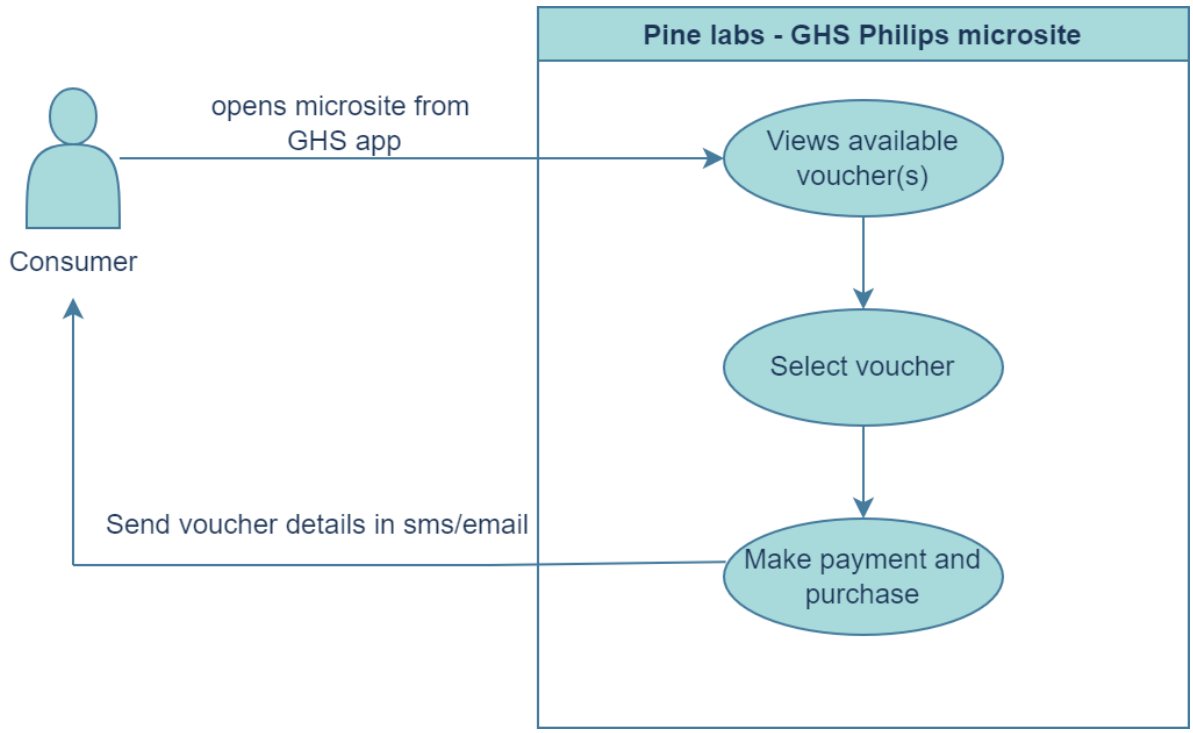
The first phase targets to provide profiler and signature journeys as service vouchers.

Consumers can purchase the voucher from pine labs microsite, which is created as merchant site for GHS Philips. user will purchase and get the service voucher code, apply it in GHS app and subscribe to Journey.

Purchasing voucher in microsite:

User purchases service voucher code from GHS Philips microsite created by Pinelabs. Pinelabs microsite sample reference URL for yatra site: Gift Cards (woohoo.in)

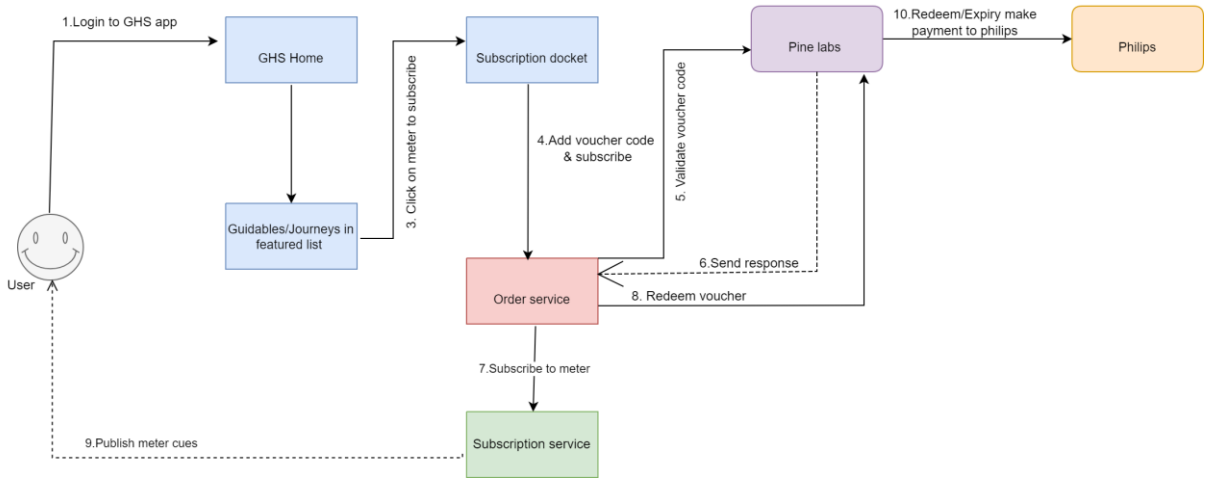
- Each service voucher code will have a prefix followed by 11-digit alphanumeric code. Example for profiler journey, Voucher code will look like: PV-1QPP-N191-0P5
- Voucher denomination is prefilled in the site



This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

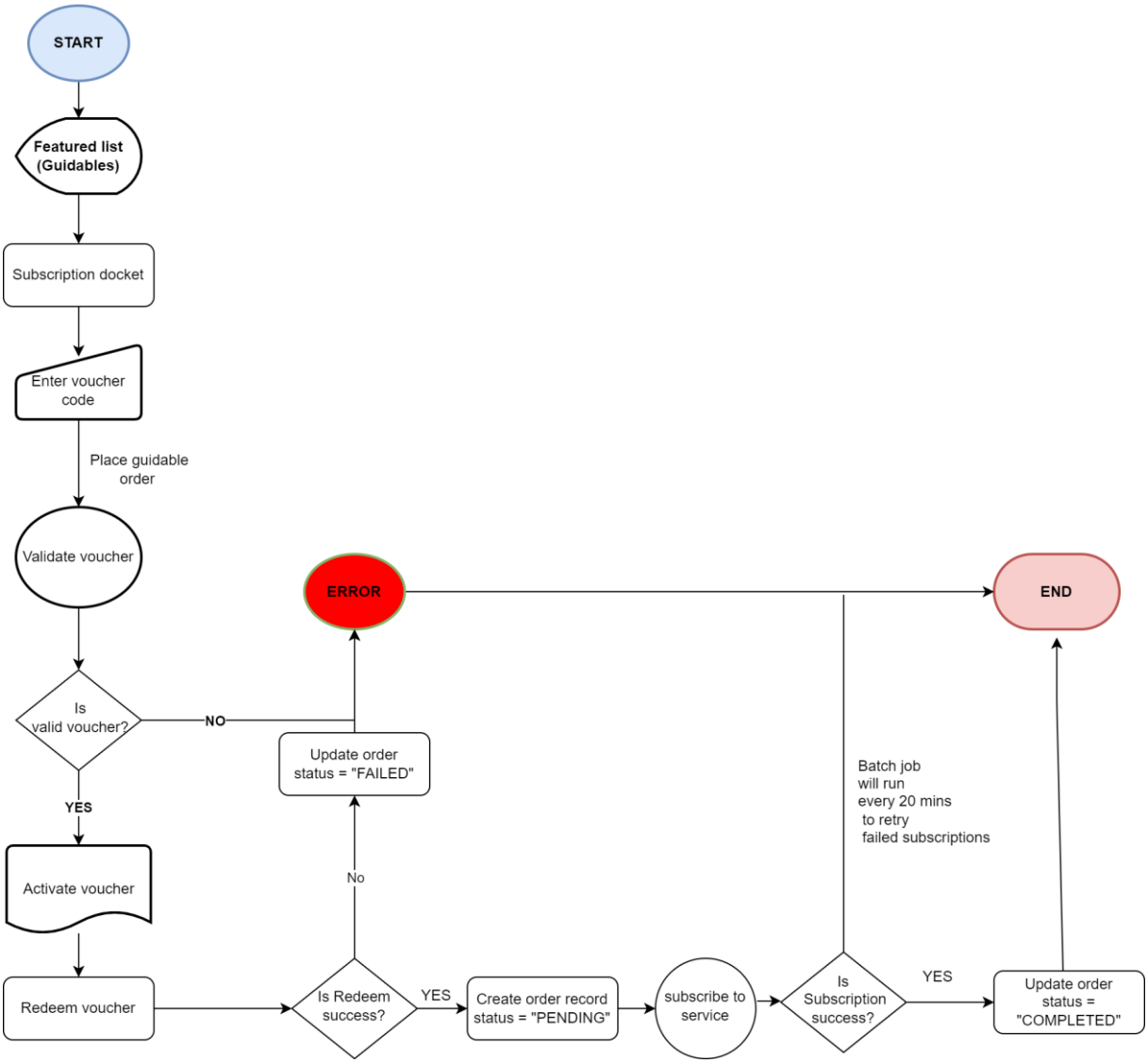
High level diagram



This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

Flow diagram



Error flow on subscription failure

- If subscription call failed, reverse voucher activation.

Error flow on redemption failure

- Batch job to run once is day to check orders with "PENDING" status and lastUpdatedOn past 1 hour and attempt redemption again.
- On successful redeem update order to "COMPLETED".

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

3. Scope

The scope of this security assessment is to perform **Grey-Box** security testing to find security threats that may come from a malicious outsider or insider user of the **GHS 1.1.5.0**. Security testing on **Web Application/Web Services** of the **GHS 1.1.5.0** is performed.

The following list includes major activities performed during the assessment:

Web Applicatin/Web Services:

1. **Webapp:** Payments Feature.
2. **Web Services/API Endpoints:**

For GHS:	1. Create order
	2. Get order
For Pinelabs:	1. Authorize
	2. Create and Issue profiler voucher
	3. Create and Issue signature voucher
	4. Activate
	5. Redeem
	6. Balance Enquiry

• Crawl through complete scope of the web application/service space and identify for any unauthenticated URL or directory.

• Check for all input injection-based attacks across all the possible entry fields in Web API.

• Exploiting any known component vulnerability or service misconfiguration.

• Reviewing the transport layer security implemented.

Follow "Test case execution" section for detailed test cases.

The test scope for this release is explained in the below table:

Type	Scope of Assessment			
Web Application	GHS	URL	https://cad-consumer-app-preint.us-east.philips-healthsuite.com/	
		Version	1.1.5.0	
		Environment	Test	
		User Role	Consumer	Can be created

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

Web Services	GHS	URL/Collection	API Collection.zip	
		Version	1.1.5.0	
		Environment	Test	
		User Role	Consumer	Available
	Pinelabs	URL/Collection	API Collection.zip	
		Version	1.1.5.0	
		Environment	Test	
		User	Internal user	Available

Not in Scope

Below mentioned items are out of scope for the current security assessment:

- Source Code Review
- Network Testing
- AI Component
- Complete Web Application Testing
- There were no payments APIs or functionality developed by GHS
- All other API's

Note: The environment provided was not stable. We have covered the testing of **GHS 1.1.5.0** in the environment provided and the results are valid if the same environment is replicated. Re-run the tests if a new propagation of the environment is made.

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

4. Executive Summary

Security Center of Excellence team engaged in activity to conduct security assessment of **GHS 1.1.5.0** which included **Web Application/Web Service** Testing in scope. The purpose of the engagement was to evaluate the security of the **GHS 1.1.5.0** against industry best practice criteria.

Note: Only highlights of important vulnerabilities are described below. Please refer 'Vulnerability Summary' section for complete detailed list of vulnerabilities.

During the security assessment of the product, security issues in the below area is found:

- Weak SSL/TLS Configuration
- Cross-origin resource sharing (CORS)
- JWT Misconfiguration
- Lack of Rate Limiting

During the security assessment of the product, security issues in the below areas were not found:

- CSRF Attacks
- Replay Attack

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

VULNERABILITY SUMMARY TABLE

The table below shows a summary of the number of vulnerabilities and their severities.

Note: The vulnerabilities mentioned in this report are technical vulnerabilities only. The Product Security Risk Assessment would report the business risks associated with these vulnerabilities.

Critical	High	Medium	Low
0	0	4	1

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

5. Vulnerability Summary

The Findings and vulnerabilities from the assessment are tabulated below

Finding No.	Vulnerability Title	Severity	Impacted Area	CVE ID*	Status
89516	Insecure CORS	Medium	Webapp & Webservices	NA	Open
89518	Lack of Resources & Rate Limiting	Medium	Webservices	NA	Open
89529	JWT Misconfiguration	Medium	Webservices	NA	Open
89522	Weak SSL/TLS Configuration	Medium	Webservices	NA	Open
89517	Improper Error Handling	Low	Webapp & Webservices	NA	Open

*CVE ID are mentioned for the vulnerabilities which has a known external CVE.

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

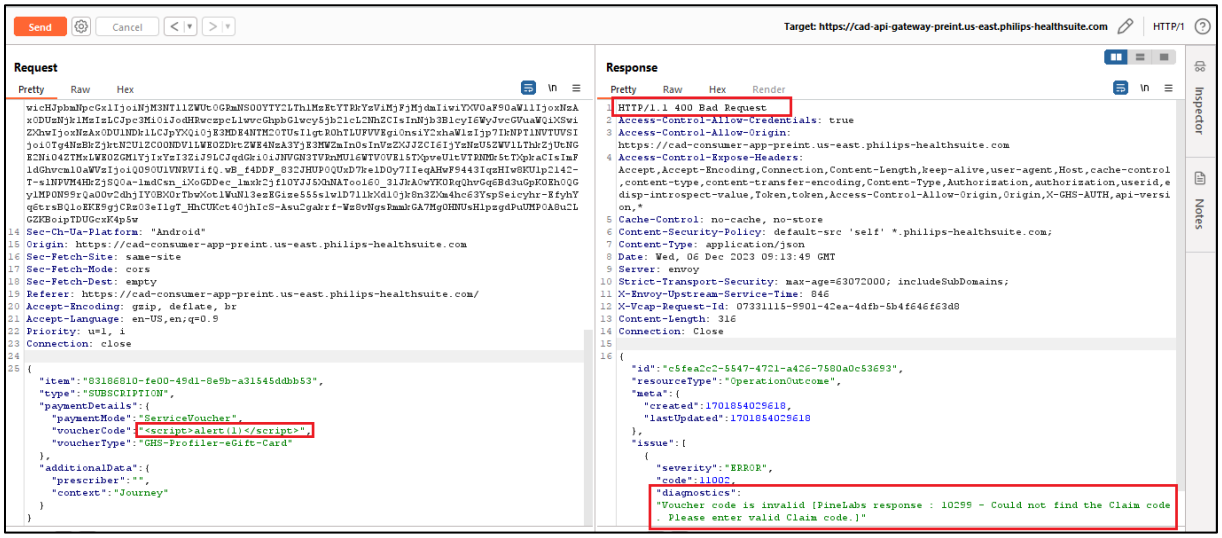
Printed copies are uncontrolled unless authenticated.

6. Observations

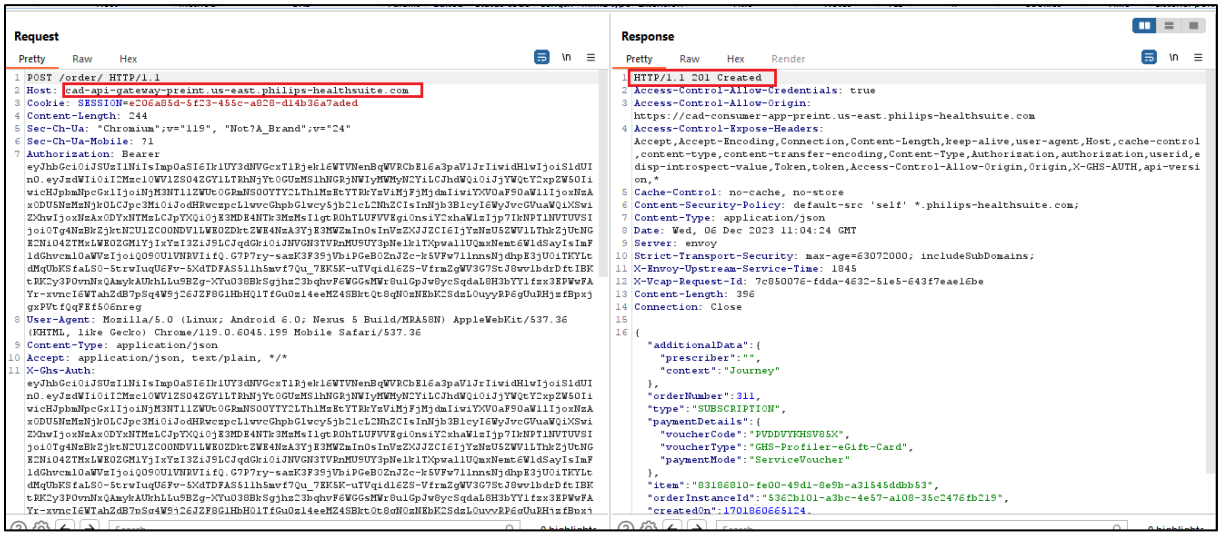
Below mentioned observations are not considered as Vulnerability but informative to the business.

Observations which shows good implementation or best practice identified:

- Input validation has been implemented on voucher code.

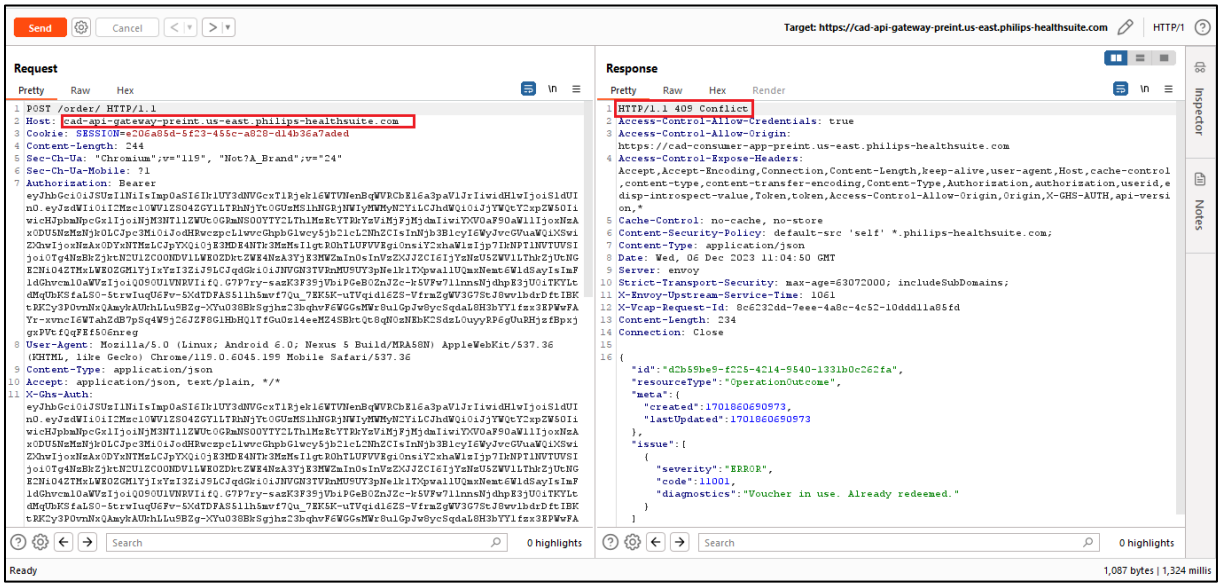


- Voucher is working for single time use only. Voucher can't be reused (Replay attack).



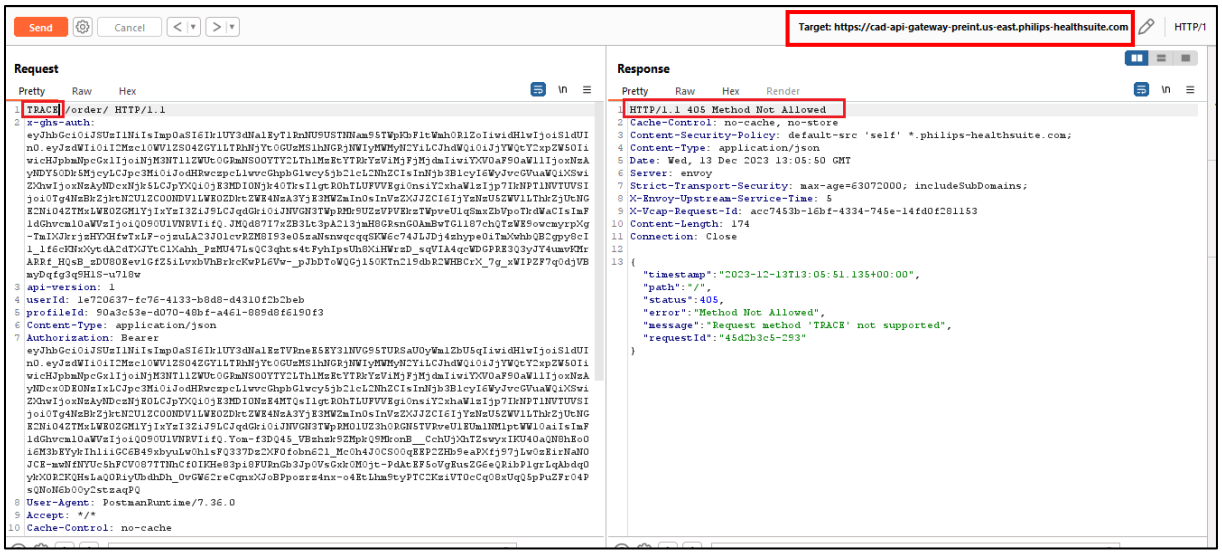
This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.



Voucher can not be reused.

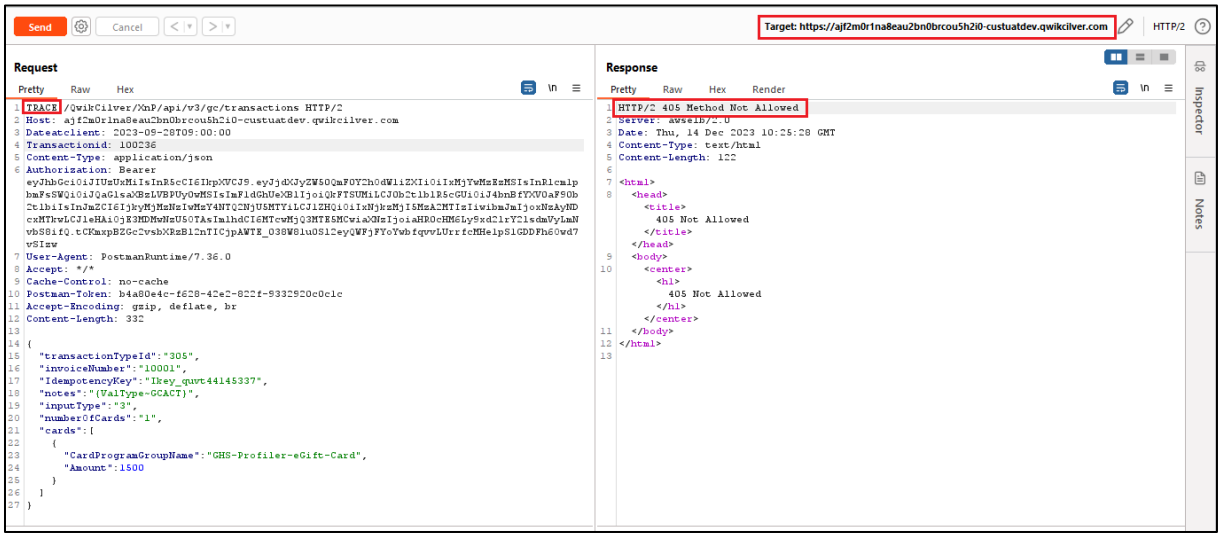
- It is observed that the endpoint is not allowing Trace method.



Webapp GHS

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

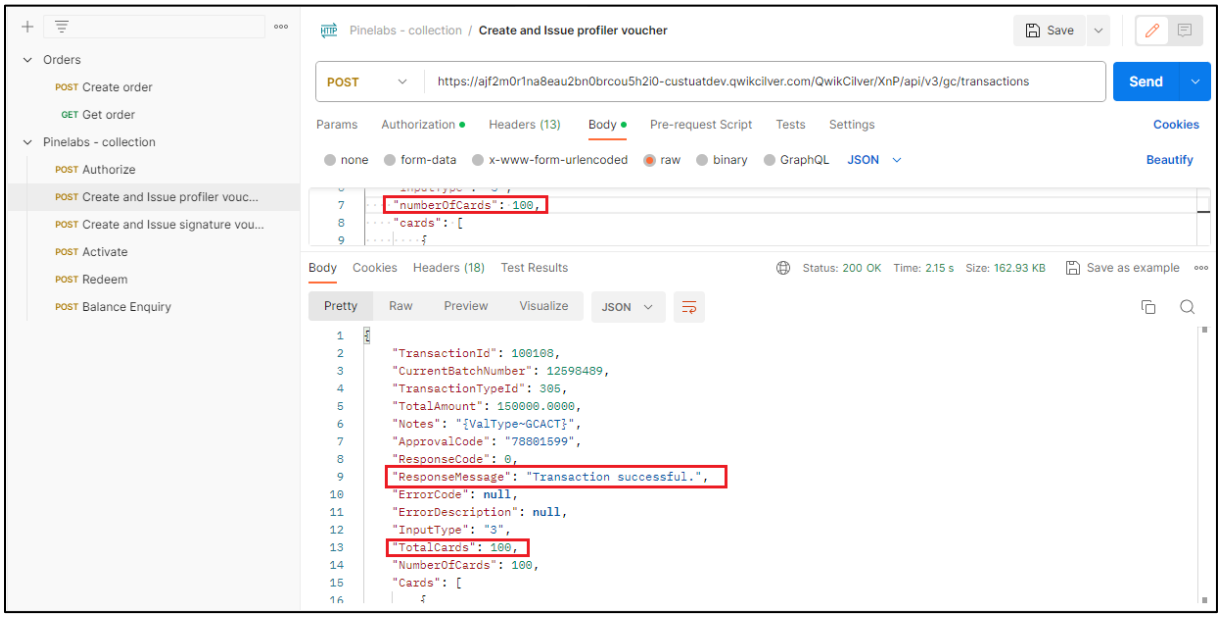
Printed copies are uncontrolled unless authenticated.



Pinelabs API

Observations which shows weak implementation are:

- In single request, we can be able to generate multiple cardpins (vouchers).



This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

7. Detailed Vulnerability Report

7.1 Webapp & Webservices: Insecure CORS

Vulnerability Title	Insecure CORS
Vulnerability Category	A5 Security Misconfiguration
Severity	**Medium**
CVSS V3 Calculation	CVSS Base Score: 6.5 CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N
Description	**Vulnerability Description** During the assessment, it is observed that the server has responded to the request with headers 'Access-Control-Allow-Origin' set to wildcard for one endpoint and google.com for other endpoint and 'Access-Control-Allow-Credentials' set to true. Cross-origin resource sharing (CORS) is a browser mechanism which enables controlled access to resources located outside of a given domain. It extends and adds flexibility to the same-origin policy (SOP). An insecure CORS configuration allows any website to trigger requests with user credentials to the target application and read the responses, thus enabling attackers to perform privileged actions or to retrieve potential sensitive information. References: • https://owasp.org/www-community/attacks/CORS_OriginHeaderScrutiny • https://www.tenable.com/plugins/was/98983 • https://developer.mozilla.org/en-US/docs/Web/HTTP/CORS **Exploitability rational** Attacker needs to be in the internal network with user privilege to carry out this attack. **Impact rational** An attacker can access sensitive data in application when server is misconfigured with CORS headers.

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

Affected Systems/IP Address/URL	Webapp: https://cad-consumer-app-preint.us-east.philips-healthsuite.com/ API (Pinelabs): https://ajf2m0r1na8eau2bn0brcou5h2i0-custuatdev.qwikcilver.com/QwikCilver/XnP/api/v3/authorize https://ajf2m0r1na8eau2bn0brcou5h2i0-custuatdev.qwikcilver.com/QwikCilver/XnP/api/v3/gc/transactions https://ajf2m0r1na8eau2bn0brcou5h2i0-custuatdev.qwikcilver.com/QwikCilver/XnP/api/v3/gc/transactions/validate API (GHS): https://cad-api-gateway-preint.us-east.philips-healthsuite.com/order/
Recommendation	The Access-Control-Allow-Origin header should not be set to a wildcard match. In most cases, this header can be safely removed. However, if the application requires a relaxation of the Same Origin Policy, the Access-Control-Allow-Origin header should whitelist only domains that are trusted by this server. Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTML5_Security_Cheat_Sheet.html#cross-origin-resource-sharing
Status	**Open**

Steps to Reproduce

Step 1: Login to the application and intercept the application traffic using web proxy tools like Burp suite.

Step 2: Send the captured request to the repeater tab.

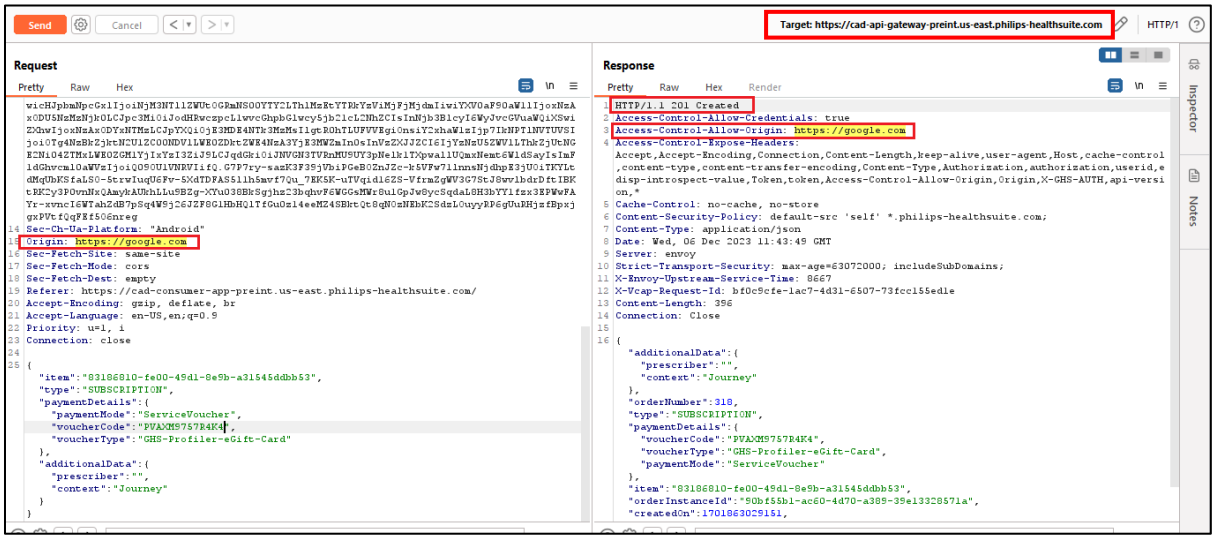
Step 3: Change the value of the origin header with any site name, e.g google.com and forward the request to server.

Step 4: Observe that the server has responded to the request with headers 'Access-Control-Allow-Origin' set to google.com and 'Access-Control-Allow-Credentials' set to true as shown in the below screenshot:

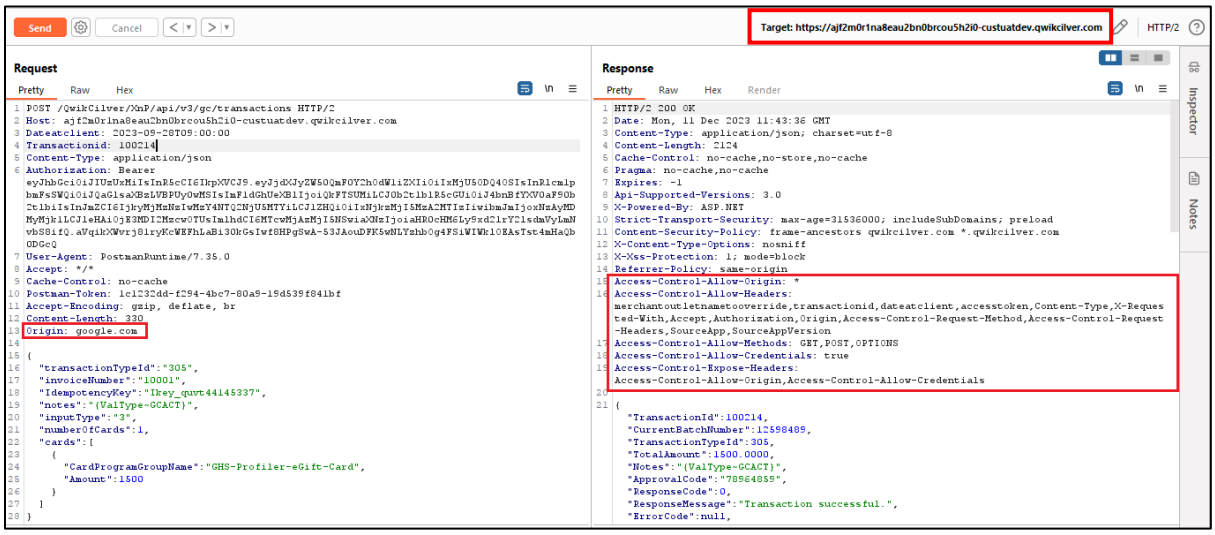
This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

Supportive Evidence:



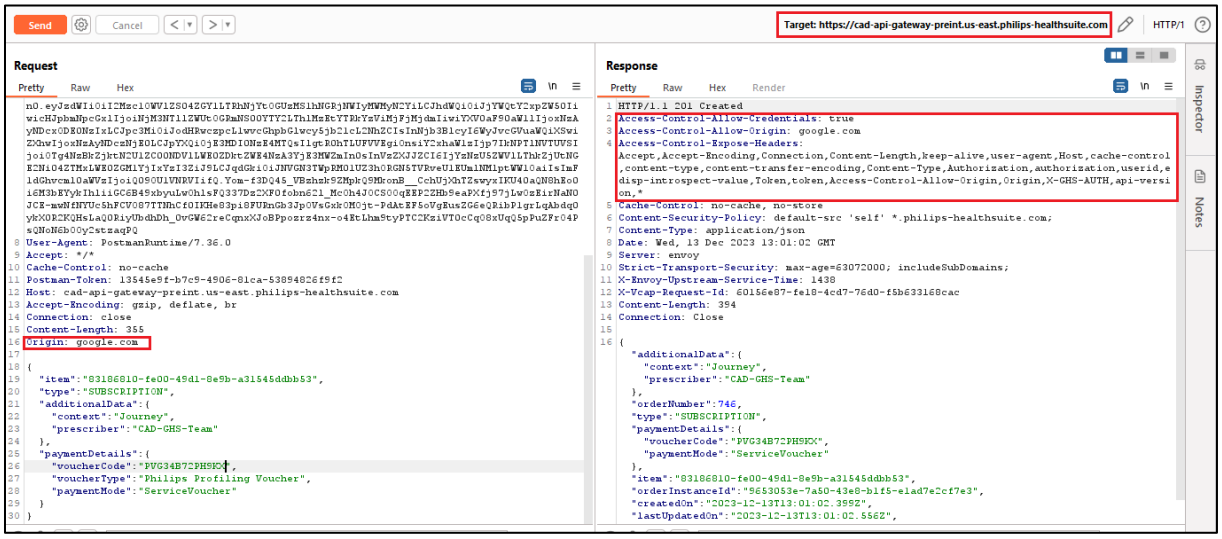
Webapp: In origin it is allowing to share its resource to google.com.



API (Pinelabs): In origin it is allowing to share its resource to 3rd party URL's.

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.



API (GHS): In origin it is allowing to share its resource to google.com.

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

7.2 Webservices: Lack of Rate Limiting

Vulnerability Title	Lack of Rate Limiting
Vulnerability Category	A5 Security Misconfiguration
Severity	**Medium**
CVSS V3 Calculation	CVSS Base Score: 5.4 CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:L
Description	**Vulnerability Description:** During security assessment, it is observed that the application has not implemented Rate Limiting on Create and Issue profiler voucher & Create and Issue signature voucher Copy requests. Rate limiting is a process to limit requests possible. It is used to control network traffic. If a web server allows upto 20 requests per minute and If you try to send more than 20 requests, an error will be triggered. This is necessary to prevent the attackers from sending excessive requests to the server. • Reduces excessive load on web servers • Prevent DOS(denial of service) attack • Help stop certain kinds of malicious bot activity like login to an account using multiple guess password and user id • Also prevent brute-force attacks API requests consume resources such as network, CPU, memory, and storage. The amount of resources required to satisfy a request greatly depends on the user input and endpoint business logic. An API is vulnerable if at least one of the following limits is missing or set inappropriately (e.g., too low/high): • Execution timeouts • Max allocable memory • Number of file descriptors • Number of processes • Request payload size (e.g., uploads) • Number of requests per client/resource • Number of records per page to return in a single request response

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

	References: Security Strategies for Microservices-based Application Systems (nist.gov) CWE - CWE-770: Allocation of Resources Without Limits or Throttling (4.10) (mitre.org) CWE - CWE-307: Improper Restriction of Excessive Authentication Attempts (4.10) (mitre.org) **Exploitability Rational** Exploitation requires simple API requests. Multiple concurrent requests can be performed from a single local computer or by using cloud computing resources. **Impact Rational** It may lead to loss of data integrity, where attacker is able to abuse the functionality. Exploitation may lead to DoS, making the API unresponsive or even unavailable.
Affected Systems/IP Address/URL	https://ajf2m0r1na8eau2bn0brcou5h2i0-custuatdev.qwikcilver.com/QwikCilver/XnP/api/v3/gc/transactions
Recommendation	• Implement a limit on how often a client can call the API within a defined timeframe. • Notify the client when the limit is exceeded by providing the limit number and the time at which the limit will be reset. • Add proper server-side validation for query string and request body parameters, specifically the one that controls the number of records to be returned in the response. • Define and enforce maximum size of data on all incoming parameters and payloads such as maximum length for strings and maximum number of elements in arrays. **References:** CheatSheetSeries/Docker_Security_Cheat_Sheet.md at 3a8134d792528a775142471b1cb14433b4fda3fb · OWASP/CheatSheetSeries · GitHub
Status	**Open**

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

Steps to Reproduce

Step 1: Configure postman to work with a proxy tool such as Burp suite.

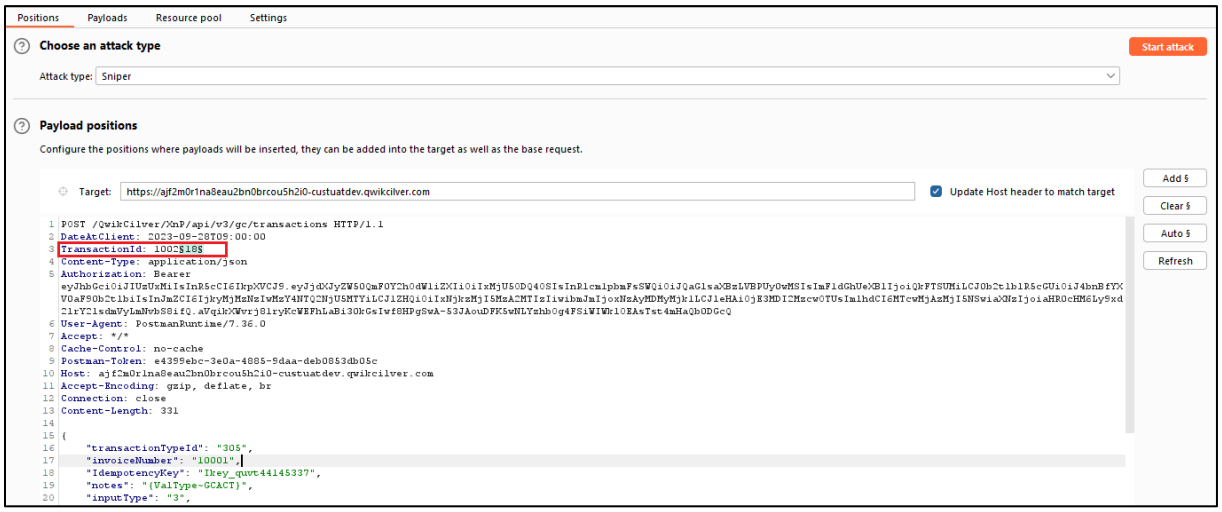
Step 2: Intercept the request Create and Issue profiler voucher & Create and Issue signature voucher Copy API.

Step 3: Send the request to intruder tab.

Step 4: Set the payload position for TransactionId parameter by incrementing 1.

Step 5: Below screenshots provides the evidences for the same.

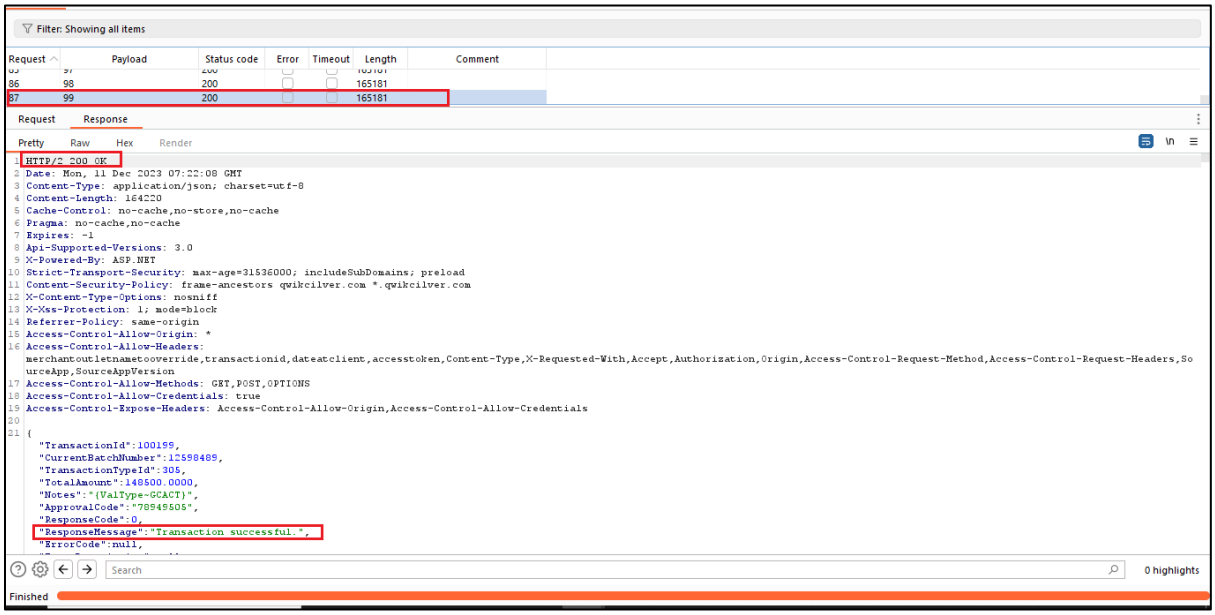
Supportive Evidence:



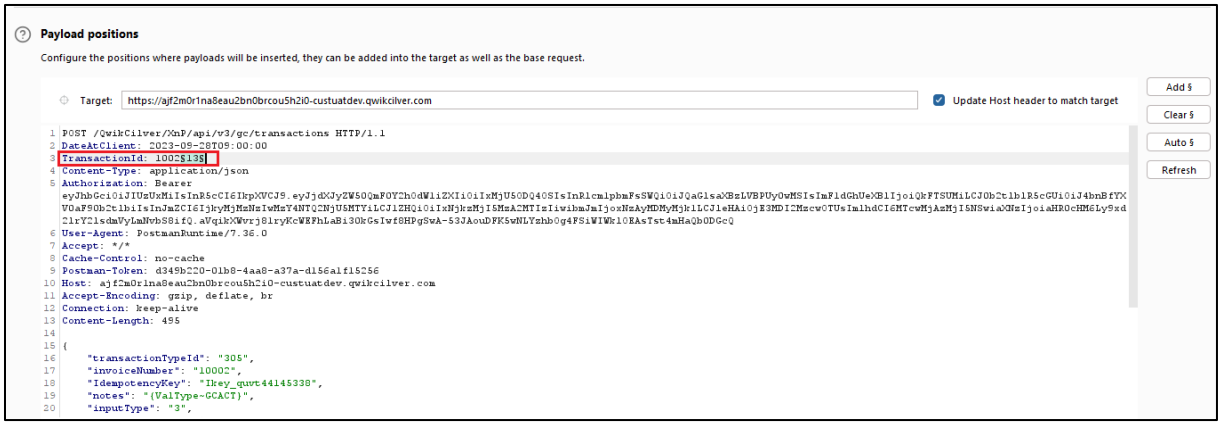
Profile Voucher: Setting payload position

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.



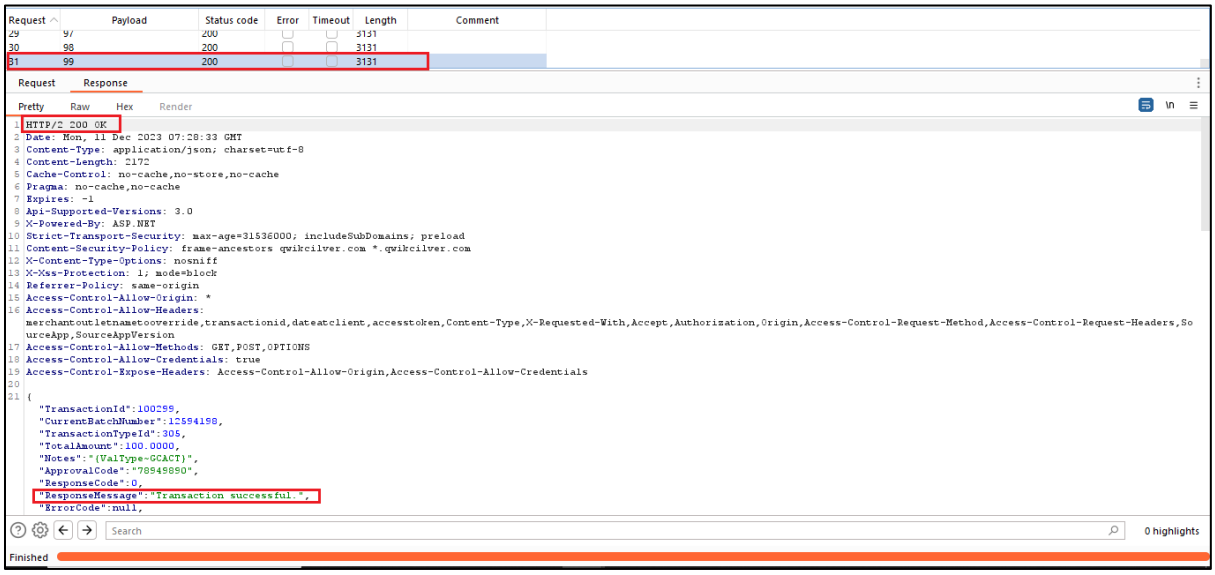
Profile Voucher: There is no rate limiting implemented.



Signature Voucher: Setting payload position

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.



Request	Payload	Status code	Error	Timeout	Length	Comment
29	97	200			3131	
30	98	200			3131	
31	99	200			3131	

Request Response

Pretty Raw Hex Render

```
1 HTTP/2 200 OK
2 Date: Mon, 11 Dec 2023 07:28:33 GMT
3 Content-Type: application/json; charset=utf-8
4 Content-Length: 2172
5 Cache-Control: no-cache,no-store,no-cache
6 Pragma: no-cache,no-cache
7 Expires: -1
8 Api-Supported-Versions: 3.0
9 X-Powered-By: ASP.NET
10 Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
11 Content-Security-Policy: frame-ancestors qwikcilver.com *.qwikcilver.com
12 X-Content-Type-Options: nosniff
13 X-Xss-Protection: 1; mode=block
14 Referrer-Policy: same-origin
15 Access-Control-Allow-Origin: *
16 Access-Control-Allow-Headers:
   merchantoutletnametooverride,transactionid,dateatclient,accesstoken,Content-Type,X-Requested-With,Accept,Authorization,Origin,Access-Control-Request-Method,Access-Control-Request-Headers,So
   urceApp,SourceAppVersion
17 Access-Control-Allow-Methods: GET,POST,OPTIONS
18 Access-Control-Allow-Credentials: true
19 Access-Control-Expose-Headers: Access-Control-Allow-Origin,Access-Control-Allow-Credentials
20
21 {
     "TransactionId":100259,
     "CurrentBatchNumber":12594198,
     "TransactionTypeId":305,
     "TotalAmount":100.0000,
     "Notes":"(ValType=GCACT)",
     "ApprovalCode":"78949890",
     "ResponseCode":0,
     "ResponseMessage":"Transaction successful.",
     "ErrorCode":null,
```

Search 0 highlights

Finished

Signature Voucher: There is no rate limiting implemented.

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

7.3 Webservices: JWT Misconfiguration

Vulnerability Title	JWT Misconfiguration
Vulnerability Category	A1 Broken Access Control
Severity	**Medium**
CVSS V3 Calculation	CVSS Base Score: 5.9 CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N
Description	**Vulnerability Description:** During the assessment, it is observed that application endpoint has implemented with JWT access token, which has long expiration time. In general, session longer then 15-30 minutes are typically considered as vulnerable. Application endpoint has token with expiry time set to 8days. JWT is an open standard (RFC 7519) for defining JSON objects shared between multiple systems and representing a user's identity or specific permission associated with that identity. JWT tokens are commonly used in authentication and authorization processes to prove a user's identity or grant access to specific protected resources or actions. **Reference:** 2020-01_Attacking_and_Securing_JWT.pdf (owasp.org) **Exploitability Rational** To exploit the vulnerability, an attacker should have network access to the server via HTTP channel. **Impact Rational** If the token has long expiration time, if the token is stolen by an attacker then the attacker can access the user's data for long period of time.
Affected Systems/IP Address/URL	Pinelabs - collection.postman_
Recommendation	It is recommended to set JWT expiration with less time period.

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

	Reference: JSON Web Token for Java - OWASP Cheat Sheet Series
Status	**Open**

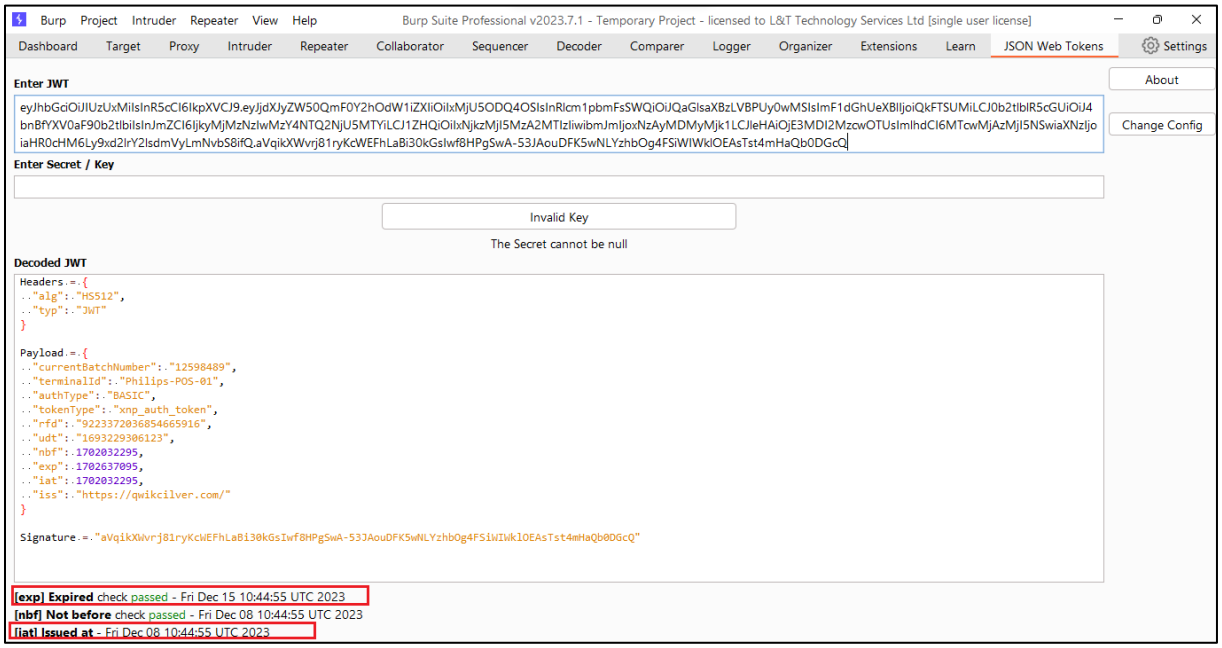
Steps to Reproduce

Step 1: Configure postman to work with a proxy tool such as Burp suite.

Step 2: Capture the request and sent to JSON web token extension.

Step 3: Observe the Issued & Expired time period.

Supportive Evidence:



Expiry time is set to 8days.

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

7.4 Webservices: Weak SSL/TLS Configuration

Vulnerability Title	Weak SSL/TLS Configuration
Vulnerability Category	A2 Cryptographic Failures
Severity	**Medium**
CVSS V3 Calculation	CVSS Base Score: 5.4 CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:N
Description	**Vulnerability Description:** During the assessment, it is observed that the application supports to use TLSv1.2 protocols but it allow weak SSL/TLS cipher suites. The server-side SSL/TLS endpoint is configured to allow weak SSL/TLS cipher suites. These cipher suites have proven cryptographic flaws that can allow an attacker to decrypt or modify traffic. These weak cipher suites include the following: * Cipher suites that use block ciphers (e.g., AES, 3DES) in CBC (Cipher Block Chaining) mode are vulnerable to the BEAST attack if SSL 3.0 or TLS 1.0 are supported. References: • https://owasp.org/Top10/A02_2021-Cryptographic_Failures/ • Weak-SSL-TLS-Ciphers-Insufficient-Transport-Layer-Protection **Exploitability rational** Some misconfigurations in the server can be used to force the use of a weak cipher or at worst no encryption - permitting to an attacker to gain access to the supposed secure communication channel. Other misconfiguration can be used for a Denial-of-Service attack. **Impact Rational** A server-side SSL/TLS endpoint that supports weak ciphers could allow an attacker to read or modify traffic sent in SSL/TLS connections with that endpoint.

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

Affected Systems/IP Address/URL	https://ajf2m0r1na8eau2bn0brcou5h2i0-custuatdev.qwikcilver.com https://cad-api-gateway-preint.us-east.philips-healthsuite.com
Recommendation	• Weak or lowgrade CBC ciphers or encryption must be disabled • *Block ciphers with key lengths of at least 128 bits (AES-128 and AES-256; optionally allow 3DES with 112-bit keys if necessary for supporting some clients) • *Block ciphers in GCM mode. Note: If CBC mode must be allowed for supporting some clients, use only CBC mode cipher suites that use the SHA2 family of hash functions (SHA256, SHA384, SHA512) Reference: https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.html
Status	**Open**

Steps to Reproduce

Use tools such as sslscan or nmap to enumerate the ciphers used by the application endpoints.

Step 1: Run the nmap scan:

nmap -p 443 -v -Pn --script ssl-enum-ciphers https://ajf2m0r1na8eau2bn0brcou5h2i0-custuatdev.qwikcilver.com

Step 2: Observe that weak ssl/tls cipher suites are allowed, as shown in the screenshot below:

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

Supportive Evidence:

```
nmap -sV -p - -Pn --script ssl-enum-ciphers ajf2m0r1na8eau2bn0brcou5h2i0-custuatdev.qwikcilver.com
|      <body>
|      <center><h1>400 Bad Request</h1></center>
|      </body>
|_     </html>
|_http-server-header: awselb/2.0
| ssl-enum-ciphers:
|   TLSv1.2:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
|       TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|     compressors:
|       NULL
|     cipher preference: server
|_  least strength: A
```

Weak CBC ciphers identified.

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

```
nmap -p 443 -v -Pn --script ssl-enum-ciphers cad-api-gateway-preint.us-east.philips-healthsuite.com
Initiating Parallel DNS resolution of 1 host. at 18:43
Completed Parallel DNS resolution of 1 host. at 18:43, 0.09s elapsed
Initiating SYN Stealth Scan at 18:43
Scanning cad-api-gateway-preint.us-east.philips-healthsuite.com (54.225.198.146) [1 port]
Discovered open port 443/tcp on 54.225.198.146
Completed SYN Stealth Scan at 18:43, 0.27s elapsed (1 total ports)
NSE: Script scanning 54.225.198.146.
Initiating NSE at 18:43
Completed NSE at 18:43, 15.18s elapsed
Nmap scan report for cad-api-gateway-preint.us-east.philips-healthsuite.com (54.225.198.146)
Host is up (0.26s latency).
Other addresses for cad-api-gateway-preint.us-east.philips-healthsuite.com (not scanned): 54.156.33.227
rDNS record for 54.225.198.146: ec2-54-225-198-146.compute-1.amazonaws.com

PORT    STATE SERVICE
443/tcp open  https
| ssl-enum-ciphers:
|   TLSv1.2:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1) - A
|       TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A
|     compressors:
|       NULL
|     cipher preference: server
|_  least strength: A

NSE: Script Post-scanning.
Initiating NSE at 18:43
Completed NSE at 18:43, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 16.82 seconds
           Raw packets sent: 1 (44B) | Rcvd: 1 (44B)
```

Weak CBC ciphers identified.

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

7.5 Webapp & Webservices: Improper Error Handling

Vulnerability Title	Improper Error Handling
Vulnerability Category	A5 Security Misconfiguration
Severity	**Low**
CVSS V3 Calculation	CVSS Base Score: 3.4 CVSS:3.1/AV:A/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:N
Description	**Vulnerability Description:** Improper handling of errors can introduce a variety of security problems for a web site. The most common problem is when detailed internal error messages such as stack traces, database dumps, and error codes are displayed to the user (attacker). These messages reveal implementation details which are supposed to be hidden. Reference: https://owasp.org/www-community/Improper_Error_Handling **Exploitability rational** An attacker should have access to the application. **Impact rational** By leveraging the verbose error an attacker can gain more information about the target which help in fine tuning his/her future attack.
Affected Systems/IP Address/URL	https://cad-consumer-app-preint.us-east.philips-healthsuite.com/ https://cad-api-gateway-preint.us-east.philips-healthsuite.com/order/
Recommendation	The application should return customized generic error messages to the user's browser. If details about the error are needed for debugging or support reasons a unique identifier may be created and displayed to the user along with the generic error message for reference. This same unique identifier can be included with the error that is logged to the server so that it can be easily correlated with the issue.

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

	References: • https://cheatsheetseries.owasp.org/cheatsheets/Error_Handling_Cheat_Sheet.html • Improper-Error-Handling-Fix-In-JAVA • Improper-Error-Handling-Fix-In-ASP.NET-Core • Improper-Error-Handling-Fix-In-SpringBoot
Status	**Open**

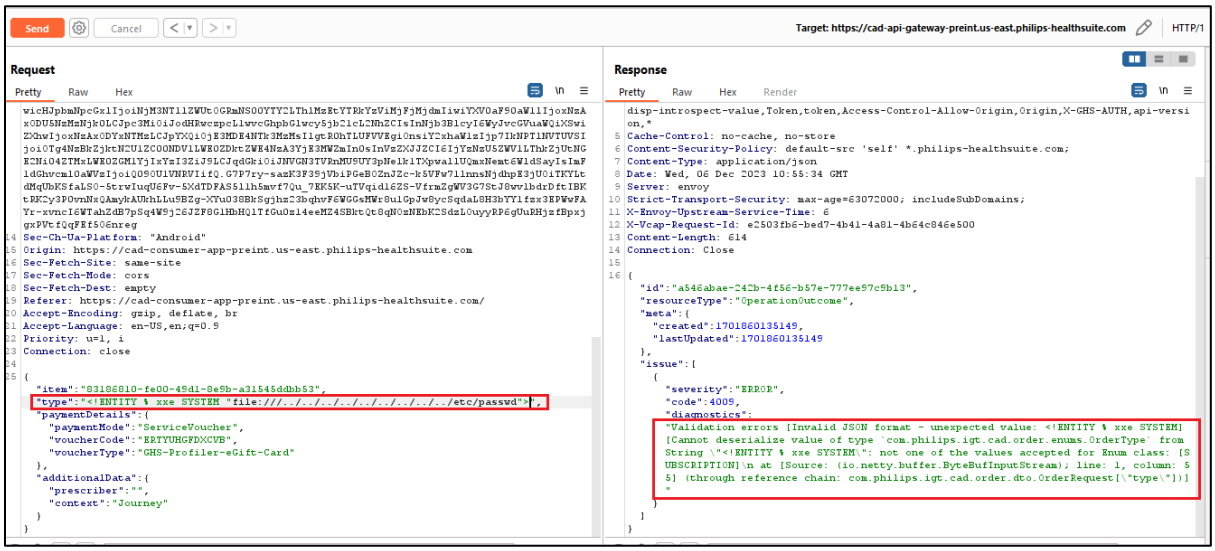
Steps to Reproduce

Step 1: Configure the browser to use proxy tool such as Burp Suite.

Step 2: Capture a request containing some input fields and send it to the Repeater tool.

Step 3: Manipulate the request with certain malicious characters in the input fields and observe that there is error disclosure in the response as shown in the screenshot below:

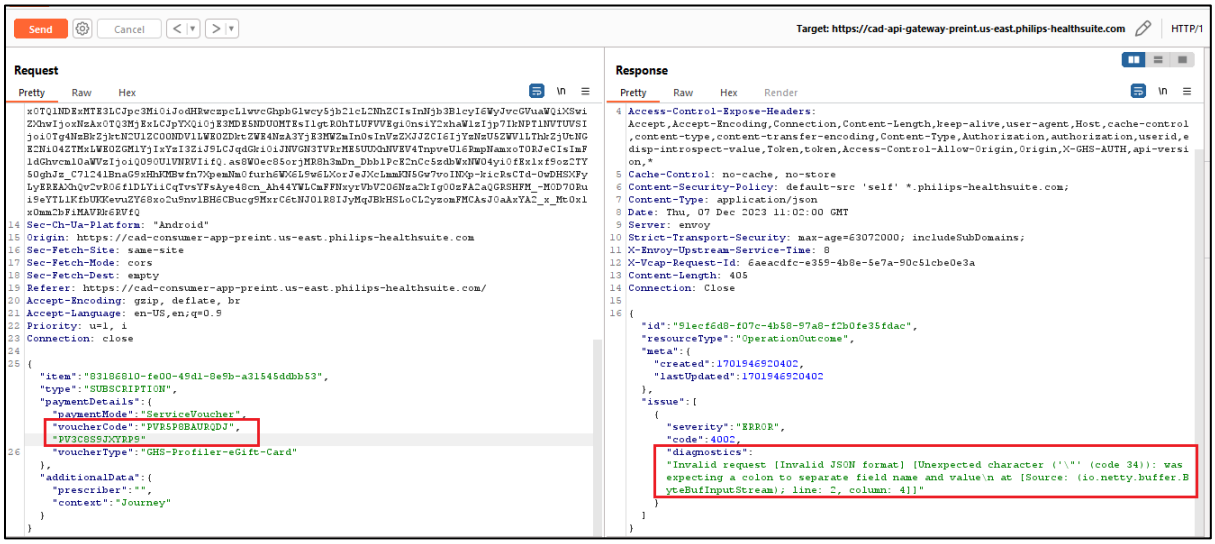
Supportive Evidence:



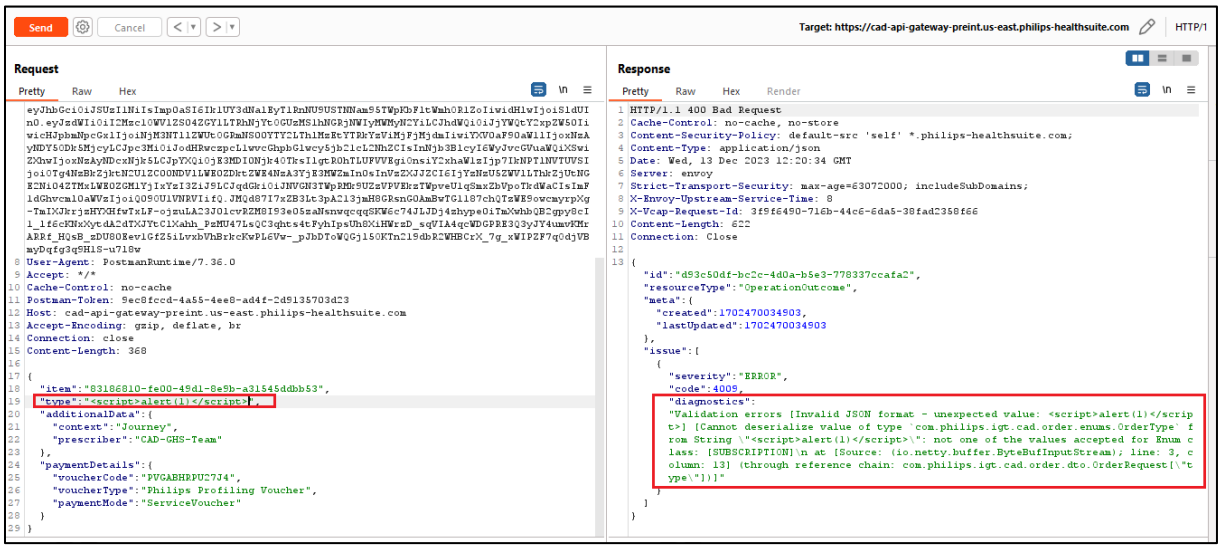
In this parameter we are passing a payload, in the response we can observe detailed error message.

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.



In this parameter we are passing a payload, in the response we can observe detailed error message.



In this parameter we are passing a payload, in the response we can observe detailed error message.

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

8. Tools Used

Scope	Tools Used
Web Application/Web Services	Burpsuite, Postman, nmap

9. Automated Tool Report

Create order nmap.txt

Pinelabs nmap.txt

10. Manual Test Reports and Test Case Execution

2850_GHS-1.1.5.0_TestSuites.xlsx

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.